Transforming Information Sharing

Improving government, public, and private partnering.

by Ms. Susan Henry
Maritime Domain Awareness Information Architect, U.S. Coast Guard

Never have the opposing needs to share and yet to protect information been greater. While government, public, and private awareness of Internet-related vulnerabilities has grown over the past decades, our lessons learned from September 11, 2001 and more recently from the Katrina disaster have made the need for expanded information sharing painfully clear. The tools of the Internet realm, balanced with due consideration of essential security, will be indispensable in creating the means for sharing information affordably between principals and stakeholders in the future, nationally and internationally.

Before we can use these tools wisely, though, we must have a broader appreciation of and knowledge about who our partners are or should be; in what situations; and what kinds of information they seek, need to protect, and can provide. Knowing this, technological tools can be applied within a logical framework.

Change at the Federal Level

For the federal government and its many departments and agencies, focusing on interagency information sharing is a monumental task. But share we must: The imperative to share information has been reinforced many times over since the Homeland Security Act of 2002, in a series of executive orders and memoranda, as well as in department directives and in public law. Originally aimed at remedying gaps in information sharing between the national intelligence community and federal law enforcement, federal attention has more recently turned to the need for stronger interagency coordination and information sharing for domestic incident management.

A new "Joint Field Office Activation and Operations Interagency Integrated Standard Operating Procedure" handbook recently received interim approval from the Department of Homeland Security (DHS). The handbook emphasized the need for information sharing between federal, state, local, tribal, and private-sector response coordinators. The mutual information sharing and information protection concerns of government and industry can not be overlooked, whether the issue at hand is counterterrorism or domestic disaster response.

Currently most of these policy references direct the sharing of information between existing organizations and their personnel, assuming the separate use of their respective centers, networks, and information systems. The emphasis is still primarily on getting communication processes between government parties right; further work remains to be done to improve communications processes with nongovernmental entities. What we have seen so far are the necessary beginnings—the policy groundwork that must be accomplished in order to improve federal information sharing.

Most of our legacy systems were not designed for the purpose of information exchange with other federal agencies, much less with non-federal organizations.

Leveraging the Legacy Infrastructure

Each department has millions, if not billions of dollars already invested in separate legacy information sys-

tems. Most of our legacy systems were not designed for the purpose of information exchange with other federal agencies, much less with nonfederal organizations. Recent policy changes and directives push us to share information, but how do we go about leveraging the legacy infrastructure?

Some small inroads toward expanded information sharing across and beyond the legacy federal infrastructure have been made. Executive Order 13356 of August 27, 2004, directed the development of common standards for information sharing, stimulating such initiatives as the National Information Exchange Model, a partnership between the Department of Justice and DHS.

DHS has deployed the Homeland Security Information Network, leveraging existing network infrastructure to provide unclassified Internet-based client-server support to federal, state, and local partners. Meanwhile, many federal departments and agencies have created Internet portals on their own, intended for the specific communities of interest they serve. Among these are the Coast Guard's Homeport, (http://Homeport.uscg.mil/) a nationwide, publicly accessible portal for federal, state, local, and industry registered users with port/maritime interests. Another example is the Environmental Protection Agency's central data exchange, or CDX, (http://www.epa.gov/cdx), with some 48,000 registered users across multiple agencies. Meanwhile, the Department of Defense (DOD) has increased its exploration of information-sharing processes and methods with non-DOD agencies and coalition partners, including extending the use of its Net-Centric Enterprise Services (NCES) to non-DOD partners. NCES supports both Internet-like information exchange and full security at multiple levels.

Federal departments and agencies are actively seeking affordable ways to share information without recapitalizing their legacy infrastructure.

In short, federal departments and agencies are actively seeking affordable ways to share information without recapitalizing their legacy infrastructure, while new collaborative policy and concepts of operations evolve in parallel. The more specifically the information needs and resources of their partners can be identified, the more quickly information sharing can be accomplished. The development of collaborative policy and concepts of operations will also provide critical justification for capital investment and resource planning. In the meantime, networked information-sharing experiments will continue at a slow pace, hampered until the value of potential partnerships is more fully understood and the supporting resources can be justified.

A New Architecture for Information Sharing

In the near future, the expansion of federal outreach to other government agencies, nongovernmental organizations, and industry partners could be greatly improved by applying service-oriented architecture (SOA) logic to our understanding of information-sharing requirements. Although there is no official single definition of SOA, this term is generally used to refer to the description of relationships between service consumers or subscribers, service providers or publishers, and on-line information technology (IT) intermediaries, including service directories and associated support (including registries and profiles, authentication, information assurance functions, and cross-domain security).

Technical execution of SOA relies heavily upon integrating web service standards and protocols, addressing technical specifications, and acquiring the ability to move data from one computer to another. Service-oriented architecture defines the business processes and services; web services are a way of enabling SOA implementation.

SOA adds a significant layer of social logic and deliberately shared implementation techniques above and beyond web services, and may include cost-sharing to accomplish community goals. The service-oriented architecture approach usually includes exploration of common vocabulary, semantic context, and meaning of the data to be shared within a given community, a subject not addressed by web services.

Prior to implementation, essential intermediary services must be identified to address quality attributes such as the security and integrity of the data, as well as access control and authentication requirements. In addition, a determination of the suitability of the legacy systems for adaptation to web services must be made within the community. SOA precepts hold that, once these architectural concerns are clarified, proven web services and other IT support can be applied more effectively, appropriately, and affordably. Cost savings may be gained from eliminating the need for point-to-point system interfaces and adaptations that might have been planned by indi-

vidual members, as well as by distributing the cost of Data Sharing over the entire community.

In the commercial IT sector, some new data service providers have completely implemented SOA principles, tracing their business lines into collaborative alliances with shared strategic goals, and implementing Internet-based technologies that best support extensible information sharing while preserving proprietary protections. Service-oriented architecture is a natural practice for a new collaborative enterprise, free of a pre-Internet legacy infrastructure.

Applying the SOA approach, or any approach, to span multiple organizations with large numbers of incompatible monolithic systems, across government, public, and private enterprises, brings with it enormous challenges. One way to begin addressing this task is to organize consumers, providers, and their information technologists into declared communities of interest (COI). These are voluntary collaborative groups that need to share information in order to accomplish shared missions, allied business processes, or other shared interests. A community of interest must first develop understanding of its mutual goals, and then resolve policy and governance issues necessary to both share and protect its information. The social network must be acknowledged and established before efficient use of IT tools can be made.

New Communities of Interest

The organization of communities of interest is a practice advocated by many leaders in government and industry, including Mr. Mike Krieger, senior executive from the DOD Chief Information Officer's staff. Following release of the federal "National Plan to Achieve Maritime Domain Awareness," Mr. Krieger briefed this practice to the interagency Maritime Domain Awareness (MDA) Implementation Team. A ground-breaking exploration of SOA across multiple agencies was subsequently launched, called the MDA Data Sharing COI (see related article in this issue). Other such communities of interest have operated under DOD guidance in past years, but this is the first such group to deliberately expand its inclusiveness into the non-DOD realm on a large scale.

To get started, this COI asked these questions:

- What organizations are interested in Maritime Domain Awareness Data Sharing?
- Which member organizations will be most active?
- What information sharing problems does this COI want to tackle?
- Which members can contribute business process knowledge, technical expertise, or funding resources?
- What data are we willing to expose and share, with what levels of protection?
- Can we agree on a data-sharing pilot that will serve a large number of the members, across differing organizations?
- Do we have legacy systems that can be easily adapted to web services and the necessary intermediary services?
- What will it cost to carry out the data-sharing pilot that we choose?

This COI's organization includes an executive-level partnership; a senior steering committee to negotiate governance issues; and working groups to compile a common vocabulary, develop a data-sharing pilot demonstration, and determine how to implement and support the pilot capability within the community. Linking the pilot to funded major system-acquisition programs is key. All of these organizational and decision process steps are consistent with SOA precepts.

The Future of Information Sharing

The same service-oriented architecture methods employed by the MDA Data Sharing COI can be used to identify, clarify, and develop solutions for information sharing across any alliance of potential government, public, and private partners. Common vocabularies already have been developed and can be leveraged by other communities, and the exploratory practices of existing collaborative alliances can serve as a model for new communities of interest.

Eventually, the use of easily extensible web services will overcome the limits of the client/server computing environment, adding layers of interoperability, while avoiding the complete redesign of legacy systems and enhancing outreach across community boundaries. The availability of intermediary support services for secure cross-community Data Sharing, such as NCES, will improve over time, as new capital investment strategies follow new collaborative policy between government, public, and private partners. The imperatives to share critical information and to protect it can and must be accomplished, for our safety, security, and survival.

About the author: *Ms. Henry is a career information architect and system engineer, specializing in the translation of requirements from operational to system levels, and is also a retired naval officer (cryptologist). She has served the Coast Guard since 1994, following previous assignments with the Navy, the Marine Corps, the U.S. Pacific Command, and the national intelligence community. Her undergraduate and graduate studies in information systems and applied mathematics were completed at the University of Hawaii.*